(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2001186122 A**

(43) Date of publication of application: **06.07.01**

(51) Int. Cl **H04L 9/32**
G09C 1/00

(21) Application number: **11363579**

(22) Date of filing: **22.12.99**

(71) Applicant: **FUJI ELECTRIC CO LTD**

(72) Inventor: **YANAGIHARA HIDEAKI**

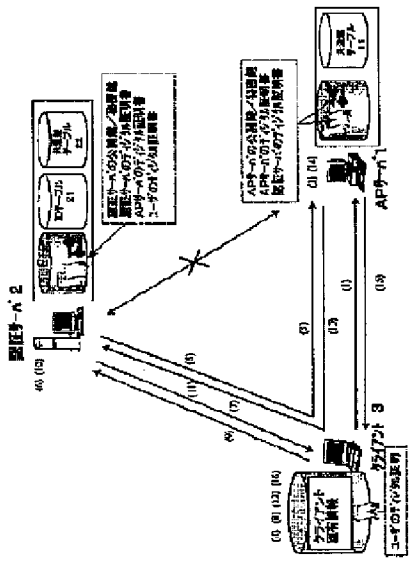
(54) AUTHENTICATION SYSTEM AND AUTHENTICATION METHOD

(57) Abstract:

PROBLEM TO BE SOLVED: To provide an authentication system that can prevent leakage of passwords and conduct retransmission of authentication data, by pretending of a 3rd party to be a legal party.

SOLUTION: When a user uses a client 3 to a log in an AP server 1, the AP server 1 generates encrypted communication data (i) and transmits the data as an authentication request to an authentication server 2 by the use of redirection through the client 3. The authentication server 2 makes request to the client 3 to enter its password and authenticates the user, on the basis of the password and the authentication request. Then the server 2 transmits encrypted communication data (iv), including the result of authentication to the AP server 1 by the use of redirection via the client 3. Furthermore, the AP server 1 generates a session ID in the case of log on of the user and registers it to a common key table 11 with a common key and detects the retransmission by comparing the ID with a session ID in the communication data (iv).

本実施形態のシステム構成を示す図



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－186122
（P2001－186122A）
(43)公開日　平成13年７月６日(2001.7.6)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/32		Ｇ０９Ｃ　1/00	６４０Ｂ	５Ｊ１０４
Ｇ０９Ｃ　1/00	６４０		６４０Ｚ	９Ａ００１
		Ｈ０４Ｌ　9/00	６７５Ｄ	
			６７５Ｂ	

審査請求　未請求　請求項の数15　ＯＬ　（全 11 頁）

(21)出願番号　特願平11－363579

(22)出願日　平成11年12月22日(1999.12.22)

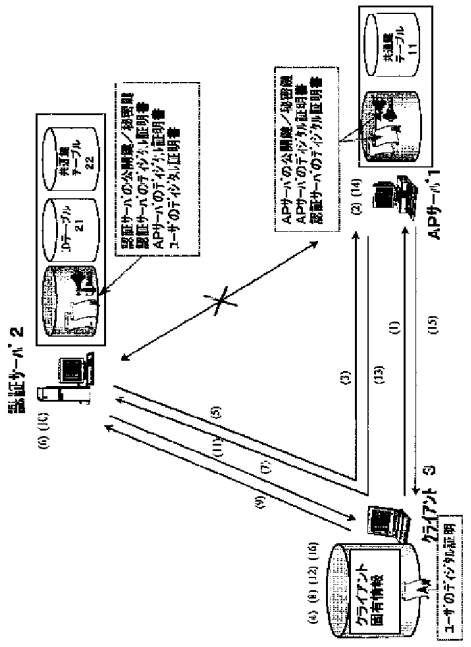
(71)出願人　000005234
富士電機株式会社
神奈川県川崎市川崎区田辺新田１番１号
(72)発明者　柳原　秀明
神奈川県川崎市川崎区田辺新田１番１号
富士電機株式会社内
(74)代理人　100074099
弁理士　大菅　義之

Ｆターム(参考)　5J104 AA07 AA08 KA01 KA05 KA06
LA02 LA03 LA05 MA02 NA05
PA07
9A001 EE03 HH33 JJ25 JJ27 KK56
LL03

(54)【発明の名称】　認証システム及び認証方法

(57)【要約】
【課題】　パスワード漏洩の防止及び第三者による成りすましを目的とした認証データの再送を防止することができる認証方式を提供することを課題とする。
【解決手段】　ユーザがクライアント３からＡＰサーバ１にログインすると、ＡＰサーバ１は暗号化した通信データ（ｉ）を生成し、これを認証依頼としてクライアント３を経由したリダイレクトを用いて認証サーバ２に送信する。認証サーバ２はクライアント３にパスワード入力を要求し、受信して認証依頼に基づいて認証を行う。そして認証結果を含む暗号化した通信データ(iv)をクライアント３を経由したリダイレクトでＡＰサーバ１に送る。またＡＰサーバ１では、ユーザのログオン時にセッションＩＤを生成して共通鍵テーブル１１に共通鍵と共に登録し、通信データ(iv)内のセッションＩＤと比較することにより再送を検出する。

本実施形態のシステム構成を示す図



【特許請求の範囲】
【請求項１】　クライアントと、認証されたユーザにサービスを提供するアプリケーションサーバ及びユーザの認証を行う認証サーバがネットワークで接続されるた認証システムにおいて、
前記アプリケーションサーバは、
アプリケーションサーバの公開鍵、アプリケーションサーバの秘密鍵及び認証サーバの公開鍵を記憶する第１の記憶手段と、
共通鍵を生成する共通鍵生成手段と、
認証対象となっているユーザのクライアントからの接続要求に対し、該クライアントの固有情報を含む認証要求メッセージ及び該認証要求メッセージのメッセージダイジェストを生成するメッセージダイジェスト生成手段と、
前記メッセージを前記共通鍵で、前記メッセージダイジェストを前記アプリケーションサーバの秘密鍵で、及び前記共通鍵を前記認証サーバの公開鍵で暗号化し、これらを認証依頼として前記認証対象となっているユーザのクライアントを介して前記認証サーバに送信する認証依頼送信手段と、
を備え、
前記認証サーバは、
認証サーバの公開鍵、認証サーバの秘密鍵及びアプリケーションサーバの公開鍵を記憶する第２の記憶手段と、
前記認証対象となっているユーザのクライアントを介して受信した前記認証依頼のうち、前記共通鍵を前記認証サーバの秘密鍵で復号化する共通鍵復号化手段と、
前記認証依頼のうち、前記共通鍵復号化手段が復号化した共通鍵で前記認証要求メッセージを、及び前記アプリケーションサーバの公開鍵で前記メッセージダイジェストを復号化する復号化手段と、
前記復号化手段が復号化した認証要求メッセージから生成したメッセージダイジェストと、前記復号化手段が復号化したメッセージダイジェストを比較して前記認証依頼の改ざんを検出する認証依頼改ざん検出手段と、
を備えることを特徴とする認証システム。
【請求項２】　前記認証サーバは、ユーザＩＤとパスワードを対応させて記憶するアカウント情報記憶手段と、前記改ざん検出手段が前記認証依頼が改ざんされていないと認定した時、前記認証対象となっているユーザのクライアントにパスワードを要求し、該クライアントからパスワードを得るパスワード取得手段と、前記認証要求内のユーザＩＤと前記パスワード取得手段が取得したパスワードの組合わせが前記アカウント情報記憶手段に記憶されていれば、認証結果として前記ユーザを認証することを示す情報を生成し、該認証結果を含む認証応答メッセージを前記認証依頼に対する応答として前記認証対象となっているユーザのクライアントを介して前記アプリケーションサーバに送信する認証結果送信手段と、を更に備えることを特徴とする請求項１に記載の認証システム。
【請求項３】　前記認証結果送信手段は、前記認証応答メッセージのメッセージダイジェストを生成し、前記認証応答メッセージを前記共通鍵で、及び前記メッセージダイジェストを前記認証サーバの秘密鍵で暗号化して、これらを前記認証依頼に対する応答として前記認証対象となっているユーザのクライアントを介して前記アプリケーションサーバに送信し、前記アプリケーションサーバは、受信した暗号化された前記認証応答メッセージを前記共通鍵で、及び前記メッセージダイジェストを前記認証サーバの公開鍵で復号化する認証応答復号化手段と、前記認証応答復号化手段が復号化したメッセージダイジェストと、前記認証応答復号化手段が復号化した前記認証応答メッセージから生成したメッセージダイジェストとを比較して前記認証結果メッセージの改ざんを検出する認証依頼改ざん検出手段と、を更に備えることを特徴とする請求項２に記載の認証システム。
【請求項４】　前記アプリケーションサーバは、前記ユーザからのログインに対してセッションＩＤを生成するセッションＩＤ生成手段と、該セッションＩＤと前記共通鍵を対応させて記憶する第１の共通鍵記憶手段と、前記セッションＩＤ生成時に前記共通鍵とセッションＩＤを前記第１の共通鍵記憶手段に記憶させ、前記認証依頼に対する応答を受信時に、該応答に含まれるセッションＩＤにより前記第１の共通鍵記憶手段から共通鍵を読み出すと共に該セッションＩＤと共通鍵を前記第１の共通鍵記憶手段から削除する共通鍵管理手段とを更に備えることを特徴とする請求項１乃３のいずれか１つに記載の認証システム。
【請求項５】　前記認証要求メッセージは前記セッションＩＤを含み、前記認証依頼送信手段は、前記認証依頼送信時、前記セッションＩＤを前記認証対象となっているユーザのクライアントに記憶させ、前記認証サーバは、前記セッションＩＤと前記共通鍵を対応させて記憶する第２の共通鍵記憶手段と、前記認証依頼受信時、該認証依頼内のセッションＩＤと前記共通鍵を前記第２の共通鍵記憶手段に記憶させ、前記認証結果送信手段が前記認証結果を送信する時、前記セッションＩＤと共通鍵を前記第２の共通鍵記憶手段から削除する再送検出手段を更に備えることを特徴とする請求項１乃至４のいずれか１つに記載の認証システム。
【請求項６】　前記認証対象となっているクライアントは、前記認証サーバからパスワードの要求が有った時、該パスワードと共に自己が記憶しているセッションＩＤを前記認証サーバに送信し、前記再送検出手段は、前記クライアントから受信したセッションＩＤにより前記第２の共通鍵記憶手段を検索して再送を検出することを特徴とする請求項５に記載の認証システム。
【請求項７】　前記アプリケーションサーバ及び認証サ

ーバは、前記第１及び第２の共通鍵記憶手段にセッションＩＤ及び共通鍵を記憶してから特定時間経過に該セッションＩＤ及び共通鍵を削除するタイムアウト手段を更に備えることを特徴とする請求項５又は６に記載の認証システム。

【請求項８】　前記認証依頼送信手段及び前記認証結果送信手段は、ＨＴＴＰのリダイレクト機能により、認証対象となっているユーザのクライアントを経由して認証サーバまたはアプリケーションサーバに認証依頼または認証結果を送信することを特徴とする請求項２乃至７のいずれか１つに記載の認証システム。

【請求項９】　前記認証対象となっているクライアントは、前記アプリケーションサーバから前記認証依頼を受信すると該認証依頼にユーザのデジタル証明書を付加して前記認証サーバに送信することを特徴とする請求項１乃至８に記載の認証システム。

【請求項１０】　前記パスワード取得手段は、前記認証対象となっているユーザのクライアントに前記ディジタル証明書内のユーザＩＤと共にパスワード要求を送信することを特徴とする請求項９に記載の認証システム。

【請求項１１】　クライアントと、認証されたユーザにサービスを提供するアプリケーションサーバと、該アプリケーションサーバからの認証依頼に対してユーザの認証を行う認証サーバとがネットワークで接続されているシステムに於けるユーザ認証方法であって、

前記アプリケーションサーバは、前記認証依頼を前記クライアントを介して前記認証サーバに行い、

前記認証サーバは、前記認証依頼に対する認証結果を前記クライアントを介して前記アプリケーションサーバに送ることを特徴とするユーザ認証方法。

【請求項１２】　前記アプリケーションサーバは、前記認証依頼に認証対象であるユーザのクライアントの固有の情報を含めることを特徴とする請求項１１に記載のユーザ認証方法。

【請求項１３】　前記アプリケーションサーバは、前記認証依頼に前記クライアントからのアクセス日時に基づく日時情報を含め、前記認証サーバは前記日時情報と現在の日時を比較することを特徴とする請求項１１又は１２に記載のユーザ認証方法。

【請求項１４】　前記アプリケーションサーバは、前記ユーザからのログインに対してユニークなＩＤを生成し、該ＩＤをキーとするテーブルに前記認証依頼の暗号化に用いた共通鍵を登録することを特徴とする請求項１０乃至１３のいずれか１つに記載のユーザ認証方法。

【請求項１５】　前記テーブルに前記共通鍵を登録してから一定期間経過後、該共通鍵を削除することを特徴とする請求項１４に記載のユーザ認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、アプリケーションのクライアント／サーバと認証サーバによって構成され、これらをネットワークで接続するシステムにおける、公開鍵暗号方式を用いた認証システム及び認証方法に関する。

【０００２】

【従来の技術】インターネットの発達によりネットワークを介した様々なサービスの提供や電子商取引が盛んになっている。この為、ネットワークを介してやり取りされるデータの機密性を確保することや、またデータが第三者によって改ざんされていないことを確認し、データの正当性、安全性を確保するための認証技術が重要になっている。

【０００３】現在一般的に行われている認証サーバを用いたユーザ認証方式を図６に示す。

【０００４】図６の構成では、ネットワークを介してクライアント１０３にサービスを提供するアプリケーションサーバ（以下ＡＰサーバという。尚以下の説明では、認証された特定ユーザに対してサービスを提供するサーバを総称してＡＰサーバという）１０１とＡＰサーバ１０１からの依頼により、ユーザの認証を行う認証サーバ１０３とがインターネットによって接続されている。また認証サーバ１０２では、ユーザＩＤとパスワードをテーブル１０４（以下、ＩＤテーブルという）にデータベース化して登録して、一元管理している。

【０００５】以下に図６を用いて従来の認証方式での動作を説明する。尚下記の説明中での(01)～(04)の番号は図６内の番号と対応している。

【０００６】クライアント１０３からユーザは、サービスを受けようとするＡＰサーバ１０１にネットワークを介してログインし、ユーザＩＤとパスワード（以下、アカウント情報という）を送信して、接続要求を行う（図６(01)）。

【０００７】ユーザからの接続要求に対してＡＰサーバ１０１は、クライアント１０３から受取ったアカウント情報を暗号化して認証サーバ１０２に送信し、認証依頼を行う（(02)）。これを受けて認証サーバは、受信したアカウント情報を用いてＩＤテーブル１０４を照合して正当なユーザであるか否かを調べ、認証結果を暗号化してＡＰサーバ１０１に返信する（(03)）。

【０００８】ＡＰサーバ１０１は認証サーバ１０２からの認証結果を元に、クライアント１０３に要求されているサービスを提供するアプリケーション画面もしくは認証エラー画面を送信する（(04)）。

【０００９】一般に認証処理においては、ネットワークを介してやり取りされる情報を各コンピュータで暗号化してアカウント情報等の漏洩防止を行っており、その場合暗号化の方法としては以下のいずれかの方式を用いている。

【００１０】(A) 共通鍵暗号方式

・送信側と受信側で固定の共通鍵を所有し、それを用い

て認証データを暗号／復号化する。
【００１１】(B) 公開鍵暗号方式
・送信側は、認証データを受信側の公開鍵で暗号化して送信する。
・受信側は、送信されてきた認証データを自分の秘密鍵で復号化する。
【００１２】(C) 共通鍵暗号方式と公開鍵暗号方式を組み合わせた方式。
・送信側は、ランダム生成した共通鍵を使って認証データを暗号化し、その共通鍵を受信側の公開鍵で暗号化（以下、ディジタル封筒という）して暗号化した認証データと共に送信する。
・受信側は、自分の秘密鍵でディジタル封筒を復号化して共通鍵を取り出し、それを使って暗号化された認証データを復号化する。
【００１３】尚(B)、(C) に関してはディジタル署名と組み合わせてデータの改ざん検出を行っている場合もある。
【００１４】
【発明が解決しようとする課題】これまでの認証方式では、以下の様な問題点がある。
【００１５】認証に用いられるパスワードは、氏名や個人情報から推測され易く、第三者に漏洩する危険性が高いうえに、ＡＰサーバ側にアカウント情報採取プログラムなどを組み込むことにより、ＡＰサーバがクライアントからアカウント情報を受信する過程において、認証に用いられるパスワード等のアカウント情報がＡＰサーバの管理者などに盗まれる可能性がある。
【００１６】また本来利用資格が無い第三者（ＡＰサーバの管理者も含む）がネットワーク盗聴などによって認証データを傍受した場合、盗聴者がそのデータを再送することにより、正当なユーザに代わってアクセス権を奪うことが出来る。
【００１７】本発明は上記問題を解消するためなされたものであり、ユーザＩＤやパスワード等のアカウント情報がＡＰサーバを経由せず認証を行うシステム及び認証方法を提供することを課題とする。また、ユーザやサーバの公開鍵証明書（以下、ディジタル証明書という）をベースとした公開鍵暗号方式とパスワードを組み合わせた認証処理を行うシステムや認証方法を提供することを課題とする。
【００１８】
【課題を解決するための手段】上記目的を達成するために、本発明による認証システムでは、クライアントと、認証されたユーザにサービスを提供するアプリケーションサーバ及びユーザの認証を行う認証サーバがネットワークで接続されるた認証システムにおいて、上記アプリケーションサーバは、第１の記憶手段、共通鍵生成手段、メッセージダイジェスト生成手段及び認証依頼送信手段を備える。
【００１９】第１の記憶手段と、アプリケーションサーバの公開鍵、アプリケーションサーバの秘密鍵及び認証サーバの公開鍵を記憶する。
【００２０】共通鍵生成手段は、共通鍵を生成する。
【００２１】メッセージダイジェスト生成手段は、認証対象となっているユーザのクライアントからの接続要求に対し、該クライアントの固有情報を含む認証要求メッセージ及び該認証要求メッセージのメッセージダイジェストを生成する。
【００２２】認証依頼送信手段は、上記メッセージを上記共通鍵で、上記メッセージダイジェストを上記アプリケーションサーバの秘密鍵で、及び上記共通鍵を上記認証サーバの公開鍵で暗号化し、これらを認証依頼として上記認証対象となっているユーザのクライアントを介して上記認証サーバに送信する。
【００２３】また上記認証サーバは、第２の記憶手段、共通鍵復号化手段、復号化手段及び認証依頼改ざん検出手段を備える。
【００２４】第２の記憶手段、認証サーバの公開鍵、認証サーバの秘密鍵及びアプリケーションサーバの公開鍵を記憶する
共通鍵復号化手段は、上記認証対象となっているユーザのクライアントを介して受信した上記認証依頼のうち、上記共通鍵を上記認証サーバの秘密鍵で復号化する。
【００２５】復号化手段は、上記認証依頼のうち、上記共通鍵復号化手段が復号化した共通鍵で上記認証要求メッセージを、及び上記アプリケーションサーバの公開鍵で上記メッセージダイジェストを復号化する。
【００２６】認証依頼改ざん検出手段は、上記復号化手段が復号化した認証要求メッセージから生成したメッセージダイジェストと、上記復号化手段が復号化したメッセージダイジェストを比較して上記認証依頼の改ざんを検出する。
【００２７】また上記認証サーバは、ユーザＩＤとパスワードを対応させて記憶するアカウント情報記憶手段と、上記改ざん検出手段が上記認証依頼が改ざんされていないと認定した時、上記認証対象となっているユーザのクライアントにパスワードを要求し、該クライアントからパスワードを得るパスワード取得手段と、上記認証要求内のユーザＩＤと上記パスワード取得手段が取得したパスワードの組合わせが上記アカウント情報記憶手段に記憶されていれば、認証結果として上記ユーザを認証することを示す情報を生成し、該認証結果を含む認証応答メッセージを上記認証依頼に対する応答として上記認証対象となっているユーザのクライアントを介して上記アプリケーションサーバに送信する認証結果送信手段とを更に備える構成とすることも出来る。
【００２８】更に認証サーバは上記認証結果送信手段が、上記認証応答メッセージのメッセージダイジェストを生成し、上記認証応答メッセージを上記共通鍵で、及

び上記メッセージダイジェストを上記認証サーバの秘密鍵で暗号化して、これらを上記認証依頼に対する応答として上記認証対象となっているユーザのクライアントを介して上記アプリケーションサーバに送信しする構成とする。そして、上記アプリケーションサーバが、受信した暗号化された上記認証応答メッセージを上記共通鍵で、及び上記メッセージダイジェストを上記認証サーバの公開鍵で復号化する認証応答復号化手段と、上記認証応答復号化手段が復号化したメッセージダイジェストと、上記認証応答復号化手段が復号化した上記認証応答メッセージから生成したメッセージダイジェストとを比較して上記認証結果メッセージの改ざんを検出する認証依頼改ざん検出手段を更に備える構成とすることも出来る。

【００２９】本発明によれば、アカウント情報はアプリケーションサーバを経由せず、アプリケーションサーバと認証サーバとの認証処理時のやり取りは全て認証対象となっているユーザのクライアントを経由して行われるので、第３者によってアカウント情報が盗まれにくい。また成りすましを目的とする認証データの再送に対して共通鍵を第１又は第２の共通鍵登録手段に登録しておくことにより検出することが出来る。

【００３０】

【発明の実施の形態】以下、本発明を図面に基づいて説明する。

【００３１】図１は、本実施形態における構成を示す図である。

【００３２】図１の構成では、ユーザ端末となる複数のクライアント３とネットワークを介してクライアント３にサービスを提供する１乃至複数のＡＰサーバ１及びＡＰサーバ１からの依頼によりユーザの認証を行う認証サーバ２とによって構成され、これらはインターネット技術を基板として構築されたネットワークによって接続されている。

【００３３】ＡＰサーバ１及び認証サーバ２は、自己の秘密鍵と公開鍵、自己及び互いのディジタル証明書を記憶している。尚このＡＰサーバ１のディジタル証明書、認証サーバ２のディジタル証明書及び後述するユーザのディジタル証明書は認証サーバ２が発行したものでも公的認証局が発行したものでもよい。

【００３４】認証サーバ２はＩＤテーブル２１を備え、このＩＤテーブル２１にユーザ認証用にアカウント情報の組み合わせをデータベース化して登録して、一元管理している。またＡＰサーバ１及び認証サーバ２は、後述する認証要求メッセージの暗号化に用いる共通鍵を登録しておく共通鍵テーブル１１、２２を備えている。更に認証処理が中断した場合などの理由で、セションＩＤと共通鍵の情報が共通鍵テーブル１１、２２中に保存されたままとなることを防ぐため、共通鍵を保存後一定時間後に共通鍵の情報を共通鍵テーブル１１、２２から削除する不図示のタイムアウトプログラム１２、２３を備えている。

【００３５】図１のシステムでは、認証処理において、認証の依頼や認証結果の返信等のＡＰサーバ１と認証サーバ２との間の認証データのやり取りにＨＴＴＰ（hyper text trnsfer protocol ）プロトコルなどに実装されている別サーバに自動的に接続するリダイレクト機能を用い、ＡＰサーバ１と認証サーバ２とで直接やり取りせず、クライアント３を経由して行うことを特徴としている。従って、アカウント情報がＡＰサーバ１に送られないので、ＡＰサーバ１側からパスワード等のアカウント情報が漏洩することはない。

【００３６】図２から図５は、認証処理における通信手順を説明したものである。以下に、図面を参照して順を追って説明する。尚下記の説明中での(1) ～(15)の番号は各認証処理を示すもので、図２乃至図４内の番号と対応している。

【００３７】図２は、図１のシステムによる認証処理のうち、ユーザがクライアント３からＡＰサーバ１にログインし、ＡＰサーバ１が認証サーバ２にそのユーザの認証を依頼するまでの処理の流れを詳細に示したものである。尚下記の説明中での(1)～(6) の番号は図２中の番号と対応している。

【００３８】まずサービスを受けようとするユーザは、クライアント３からネットワークを介してＡＰサーバ１にログインして接続要求を行う（(1) ）。この際、クライアント３はＩＰアドレスなどのクライアント固有の情報（以下クライアント固有情報という）をＡＰサーバ１に送信する。

【００３９】ＡＰサーバ１では、クライアント３からの接続要求に対して、認証サーバ２にこのユーザの認証の依頼を行う認証通信データ（ｉ）を生成し（(2) ）、これをクライアント３に返信する（(3) ）。

【００４０】図３は、ＡＰサーバ１で行われる通信データ（ｉ）の生成の流れを示す図である。

【００４１】ＡＰサーバ１では、クライアント３がログインすると、セションＩＤを生成する。このセッションＩＤは、ＡＰサーバ１に設定されるセッションを一意に識別する識別子で例えば接続要求を受け付けた時刻などを元にして生成したユニークな文字列を用いてもよいし、或は接続要求が有った順に順次符号を割付けてもよい。

【００４２】次にＡＰサーバ１は、このセションＩＤ、アクセス日時、クライアント固有情報、及びＡＰサーバ名、ＵＲＬなどのＡＰサーバ固有の情報からなる認証要求メッセージを生成する。そしてこの認証要求メッセージに対し、ハッシュ関数を用いてメッセージダイジェストを生成し、これをＡＰサーバ１の秘密鍵で暗号化してディジタル署名とする。また認証要求メッセージをランダム生成した共通鍵を使って暗号化する。この共通鍵は

ＡＰサーバ１のメモリ、ハードディスクまたはＩＣカードなどの記憶媒体上に作成した、セションＩＤをキーとした共通鍵テーブル１１に保存する。この時に、認証処理が中断した場合などの理由で、セションＩＤと共通鍵の情報がＡＰサーバ１の記憶媒体中に保存されたままとなることを回避するため、ある一定時間後に共通鍵テーブル１１から共通鍵の情報を削除する不図示のタイムアウトプログラム１２を起動する。

【００４３】次に認証サーバのディジタル証明書内の認証サーバ２の公開鍵で、認証要求メッセージの暗号化に用いた共通鍵を暗号化してディジタル封筒を生成する。

【００４４】そしてＡＰサーバ１は、これらのデータのうちセションＩＤをクッキーとして、また暗号化した認証要求メッセージとそのディジタル署名及びディジタル封筒をＵＲＬ付加情報として、認証サーバ２へのリダイレクト命令を設定した通信ヘッダデータと一緒にクライアント３に通信データ（ｉ）として送信する（(3)）。この様に本実施形態では、ＷＷＷ（World Wide Web）のクッキー技術により、セションＩＤはクライアント３側の記憶媒体に保存されるので、セションＩＤがどのクライアントに対して発行されたものかを示す情報をＡＰサーバ１では管理していない。従って、第三者に共通鍵テーブル１１の内容を盗まれてもこれから認証対象のユーザを特定することは出来ない。

【００４５】通信データ（ｉ）をＡＰサーバ１から受信すると、クライアント３ではクッキーとして送信されたセションＩＤがクライアント３のメモリ等の記憶媒体に保存される。またクライアント１は、通信データ（ｉ）のヘッダのリダイレクト命令に従い、ＨＴＴＰプロトコルなどに実装されているリダイレクト機能により認証サーバ２に接続する。そして、通信データ（ｉ）のＵＲＬ付加情報として送信されてきた暗号化された認証要求メッセージとそのディジタル署名及びディジタル封筒に加え、クライアント３が持つユーザのディジタル証明書とクライアント３のクライアント固有情報をＳＳＬ（Secure Socket Layer ）などによる暗号方式を用いて暗号化して通信データ(ii)を生成し（(4)）、これを認証サーバ２に送信する（(5)）。

【００４６】通信データ（ii）を受信した認証サーバ２では、改ざんの検出等この通信データ(ii)そのものの信頼性に対する検証を行う（(6)）。

【００４７】認証サーバ２では、まずユーザのディジタル証明書内に含まれる有効期限や発行元などの情報を元に、このディジタル証明書が有効なものであるか検証を行う。これによって認証対象のユーザが正式なユーザかどうか判別が行える。

【００４８】次に、ディジタル封筒を認証サーバ２の秘密鍵で復号化し、認証要求メッセージの暗号化に用いた共通鍵を取り出す。そしてこの共通鍵で暗号化された認証要求メッセージを復号化し、クライアント固有情報やＡＰサーバ名、ＵＲＬなどのＡＰサーバ固有の情報、アクセス日時、セッションＩＤを得る。また共通鍵はセションＩＤを検索キーとして共通鍵テーブル２２に保存する。

【００４９】次にディジタル署名をＡＰサーバのディジタル証明書内のＡＰサーバ１の公開鍵で復号化して認証要求メッセージのメッセージダイジェストを取りだす。そして、これを先に復号化した認証要求メッセージに対してＡＰサーバ１と同じハッシュ関数を用いて生成したメッセージダイジェストと比較して、両者が一致しなければ、受信データはＡＰサーバ１から送信された認証データが認証サーバ２に届くまでの(3) から(5) の過程で改ざんされていることとなる。この様に暗号化されて送信されてきた認証要求メッセージから生成したメッセージダイジェストと、送信前に送信元であるＡＰサーバ１で（過程(2) で）生成されたメッセージダイジェストを比較することによって、途中で送信データの改ざんが行われていないかを判別することが出来る。

【００５０】デジタル署名を復号化したメッセージダイジェストと、認証要求メッセージから生成したメッセージダイジェストが一致したら、認証サーバ２では、次に共通鍵により復号化した認証要求メッセージからクライアント３固有の情報を取り出し、これを(4) の過程で生成されたクライアント３の固有情報と照合し、通信データ(ii)が別のクライアント３から偽って送信したものでないか判別する。また復号化した認証要求メッセージからアクセス日時（(2) の過程で生成）を取り出し、これを現在の日時と比較する。これにより過去の認証で用いた古い通信データ(ii)を同じクライアント３から再送していないか判別する。なおこの時ＡＰサーバ１と認証サーバ２の基準となる時刻にずれが生じている場合があるので、ある程度の時刻に差があっても問題なしとする。またこの時に、認証処理が中断した場合などの理由で、セションＩＤと共通鍵の情報がＡＰサーバ１の記憶媒体中に保存されたままとなることを回避するため、ある一定時間後に共通鍵テーブル２２から共通鍵の情報を削除する不図示のタイムアウトプログラム２３を起動する。

【００５１】図４は図１のシステムによる認証処理のうち、認証サーバ２が通信データ(ii)を受信後、認証サーバ２とクライアント３の間での処理の流れを詳細に示した図である。下記の説明中での(7) ～(9) の番号は図４中の番号と対応している。

【００５２】上記(6) の過程の各検証で、認証サーバ２が受信した通信データ(ii)に改ざん等が検出されず信頼がおけるものと認定されれば、次に認証サーバ２はこの通信データ(ii)から得たデータを用いてクライアント３上のユーザに対するユーザ認証を行う。

【００５３】まず認証サーバ２は、クライアント３に対してパスワード入力のためのログイン画面のデータをＳＳＬなどによる暗号方式を用いて送信し、パスワードの

入力を要求する（(7)）。この際、ユーザ証明書に含まれていたユーザＩＤを用いて、ログイン画面には既にユーザＩＤを入力済みの状態として送信する。これにより、ユーザはユーザＩＤを入力する手間が省ける。

【００５４】このデータが送信されクライアント３側にログイン画面が表示されると、ユーザは画面上からユーザ認証の為のパスワードを入力し、記憶媒体中にクッキーとして保存されているセッションＩＤと共にＳＳＬなどの暗号方式を用いて認証サーバ２に送信する（(9)）。

【００５５】認証サーバ２では、クライアント３から受信したセションＩＤを検索キーとして共通鍵テーブル２２を検索し、対応する共通鍵が共通鍵テーブル２２に登録されているかどうかを検証する。これにより、現在認証処理中の通信であることを判別出来、このセッションＩＤとパスワードが認証対象としているユーザ以外から送信されたものでないことを確認する。

【００５６】次に認証サーバ２は、クライアント３から受信したパスワードとユーザＩＤを元にＩＤテーブル２２を照合し、認証対象となっているユーザが正当なユーザであるかを判別する。その結果、クライアント３から送信されてきたユーザＩＤ及びパスワードと同じ組合わせのものがＩＤテーブル２１に登録されていれば、このユーザは正当なユーザであるとして認証許可し、逆に対応するものがＩＤテーブル２１に登録されていなければ再度ログイン画面のデータをクライアント３に送信してパスワードの入力を求める。

【００５７】図５は、図１のシステムによる認証処理のうち、クライアント３からパスワードを認証サーバ２へ送信後の処理の流れを詳細に示した図である。以下の説明中での(10)～(16)の番号は図５中の番号と対応している。

【００５８】ユーザに対する認証が終了すると認証サーバ２は、認証結果をＡＰサーバ１に通知する通信データ(iii)を生成し（(10)）、クライアント３に送信する（(11)）。

【００５９】認証サーバ２による通信データ(iii)の生成は以下の様にして行われる。

【００６０】まず認証サーバ２は、上記した種々の検証結果に基づいた、ユーザに対する認証結果及びユーザ情報等からなる認証応答メッセージを生成する。そしてこの認証応答メッセージのメッセージダイジェストをハッシュ関数により生成し、これを認証サーバ２の秘密鍵で暗号化してディジタル署名を生成する。また共通鍵テーブル２２に登録しておいた共通鍵を用いて認証応答メッセージを暗号化する。そしてこの暗号化した認証応答メッセージとそのディジタル署名をＵＲＬ付加情報とし、通信ヘッダ部分にＡＰサーバ１へのリダイレクト命令を設定したもの通信データ(iii)として生成し、これをクライアント３に送信する。

【００６１】また通信データ(iii)の送信後、この認証処理に用いた共通鍵を共通鍵テーブル２２から削除する。これにより、以降第三者の成りすまし等によって同じ共通鍵による通信データ(ii)がクライアント３から再送されてきても、これによって正当なユーザとして認証してしまうことはない。

【００６２】この通信データ(iii)を受信するとクライアント３は、そのヘッダ部分のリダイレクト命令に従ってＡＰサーバ１に接続する（(12)）。そして通信データ(iii)に付加している暗号化された認証応答メッセージ及びそのディジタル署名と共に自己の記憶媒体にクッキーとして記憶しているセションＩＤを通信データ(iv)としてＡＰサーバ１に送信する（(13)）。

【００６３】クライアント３から通信データ(iv)を受信すると、ＡＰサーバ１はこの通信データ(iv)内の認証サーバ２による認証結果に基づいて、ユーザを認証するかどうかを決める（(14)）。

【００６４】ＡＰサーバ１では、受信した通信データ(iv)から以下の様にして正当なユーザとして認証するかどうかの判断を行う。

【００６５】まず、通信データ(iv)内のセッションＩＤを用いて共通鍵テーブル１１を検索し、対応する共通鍵が共通鍵テーブル１１に登録されているか調べる。この結果、共通鍵テーブル１１に対応するセッションＩＤと共通鍵の組合わせが登録されていればまだ認証処理が完了していないユーザについての認証結果を含む通信データ(iv)であると判断出来、また対応するものが共通鍵テーブル１１に登録されていなければ、第三者がなり代わりを目的として古い通信データ通信データ(iv)を再送してきたものと判断することが出来る。

【００６６】次に共通鍵テーブル１１より取り出した共通鍵で暗号化された認証応答メッセージを復号化する。またディジタル署名を認証サーバ２の公開鍵で復号化し、先に復号化した認証要求メッセージのメッセージダイジェストと比較し、(11)から(13)の過程で内容が改ざんされていないかを判別する。

【００６７】上記した検証で問題が無ければ、受信した通信データ(iv)内に格納されている認証サーバ２による認証結果は正当なものであるので、ＡＰサーバ１は、復号化した認証応答メッセージより認証サーバ２による認証結果を取り出し、この認証結果がユーザを認証することを示すものであればユーザから要求のあるサービスに対応するアプリケーション画面を、またユーザを認証しないことを示すものであればユーザが認証されなかったことを通知するエラー画面のデータをクライアント３に送信する（(15)）。又この時、クライアントに送信するデータに、クライアント３にクッキーとして保存しておいたセションＩＤを消去する命令を通信ヘッダに設定しておく。

【００６８】この送信処理後、ＡＰサーバ１は、暗号化

に用いた共通鍵を共通鍵テーブル１１より消去し、以降同一の通信データ(iv)がクライアント３から再送されてもこれによりユーザを認証することがないようにする。

【００６９】ＡＰサーバ１からアプリケーション画面若しくはエラー画面のデータを受信したクライアントは、これを画面表示すると共に、自己の記憶媒体に中にクッキーとして保存されているセションＩＤを削除する。

【００７０】この様に本嫉視形態のシステムでは、ユーザのアカウント情報は、一切ＡＰサーバ１には送信されない。この為、第３者が、ＡＰサーバ１に何等化の仕掛けを行っても、アカウント情報をてに入れることは出来ない。また、認証の為の情報のやり取りは、全て認証対象となっているユーザの端末であるクライアント３を介して行うこととなる。よって、盗聴を行う場合は、セキュリティレベルの高い認証サーバ２や特定が困難なクライアント３に対して非常に困難である。更にＡＰサーバ１及び認証サーバ２では、認証処理時に各自の共通鍵テーブル１１、２２のチェックを行うので、第三者による過去の通信データを再送に対しても対応することが出来る。

【００７１】

【発明の効果】以上説明したように、本発明による認証システムを用いれば、認証処理時にやり取りされるユーザＩＤやパスワード等のアカウント情報はＡＰサーバを経由しないので、たとえＡＰサーバ側でデータの漏洩やネットワーク盗聴が行われても、第三者にアカウント情報が洩れることは無い。

【００７２】またユーザ認証にディジタル証明書を用いることができるので、より高い認証レベルを実現することが出来る。

【００７３】更には、認証処理時に共通鍵を生成してこれを登録しておき、認証処理完了後これを削除するので、第三者による成りすましを目的とした認証データの再送に対しても対応することが出来る。

【００７４】また認証処理時に、ユーザがユーザＩＤの入力を不要とする構成とすることが出来、ユーザの負荷軽減することが出来る。

【図面の簡単な説明】

【図１】本実施形態に於けるシステム構成を示す図である。

【図２】ユーザがログインしてから、ＡＰサーバが認証サーバに認証を依頼するまでの処理の流れを詳細に示した図である。

【図３】ＡＰサーバで行われる通信データ（ｉ）の生成の流れを示す図である。

【図４】通信データ(ii)を受信後、認証サーバとクライアントの間で行われる処理の流れを詳細に示した図である。

【図５】クライアントからパスワードを認証サーバへ送信後の処理の流れ詳細に示した図である。

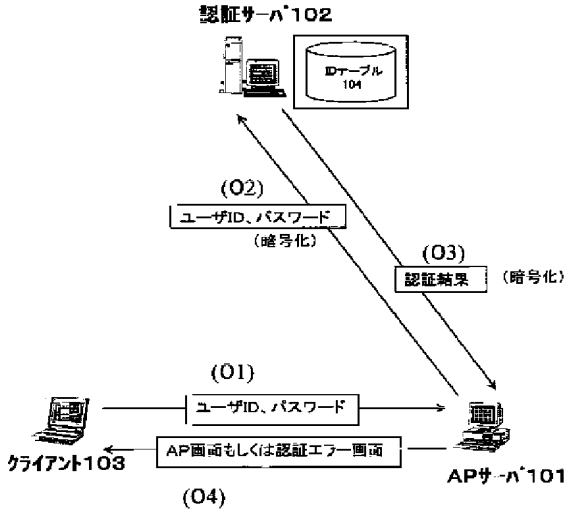
【図６】一般的に行われている認証サーバを用いたユーザ認証方式を示す図である。

【符号の説明】

１、１０１　ＡＰサーバ
２、１０２　認証サーバ
３、１０３　クライアント
１１、２２　共通鍵テーブル
２１、１０４　ＩＤテーブル

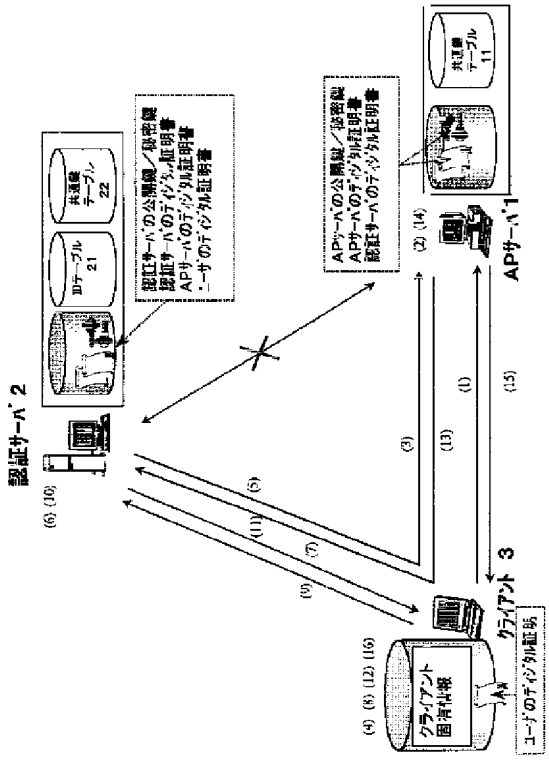
【図６】

一般的に行われている認証サーバを用いた
ユーザ認証方式を示す図



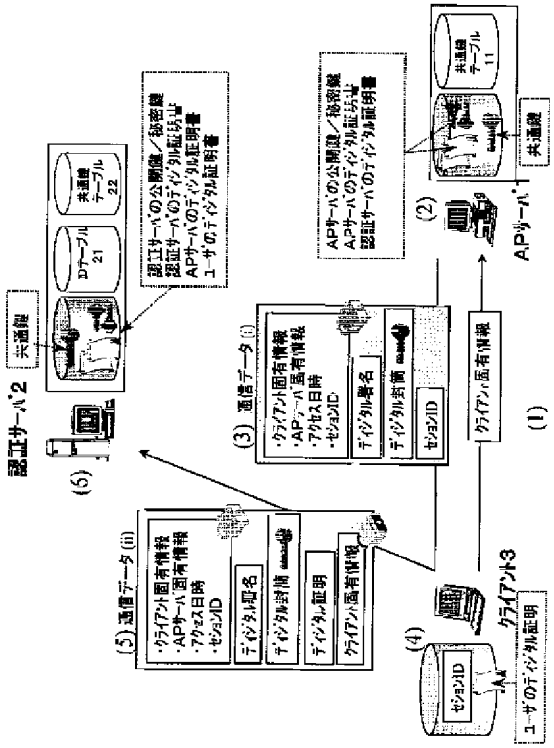
【図1】

本実施形態のシステム構成を示す図



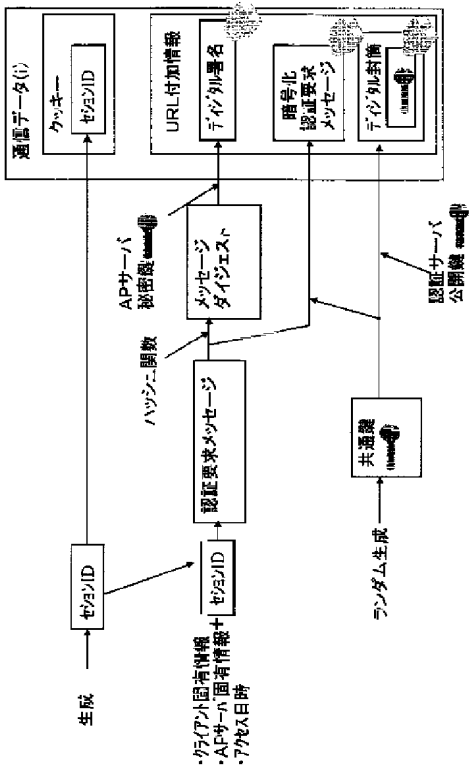
【図2】

ユーザがログインしてから、APサーバが認証サーバに認証を依頼するまでの処理の流れを詳細に示した図



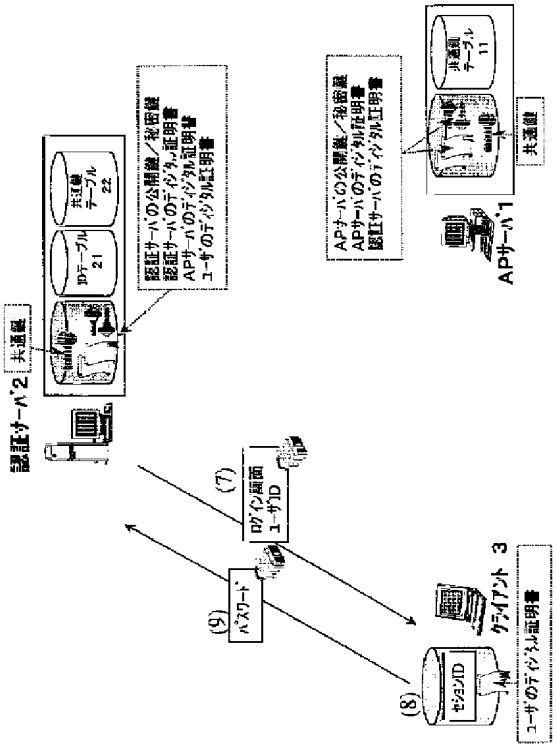
【図3】

通信データ(i)の生成の流れを示す図



【図4】

通信データ(ii)を受信後、認証サーバとクライアントの間で行われる処理の流れを詳細に示した図



【図５】

クライアントからパスワードを認証サーバへ
送信後の処理の流れを詳細に示した図